It is the assumption that kills you

John Stoop, Kindunos Safety Consultancy Ltd, Stoop@Kindunos.nl
and affiliated PhD graduate references

Abstract

This contribution reflects on the development of safety science in transport, infrastructure and logistics over a period of 40 years at Dutch universities, professional safety institutes and international networks. The contribution heavily relies on the work of the successive ESReDA Working Groups on safety investigation, the transport safety domain as deployed at Lund University in Sweden, the Delft University of Technology and the University of Applied Sciences in Amsterdam. Resulting in a series of graduate student projects, PhD studies and the author's participation in the international aviation investigation community. This contribution identifies the cornerstones for a generative design perspective, challenging a paradigm shift in safety thinking. Four new tools are introduced, materializing this challenge. Based on initial developments in aviation, maritime and agriculture, these notions are extrapolated to wind farming applications in particular in view of the EU Directive (EU) 2022/2557 on the resilience of critical entities (EU 2024).

1 Introduction

Safety and risk management heavily rely on past performance. The experience, tacit knowledge, expertise and best practices gained in the past, invite to extrapolate existing risk and safety notions and strategies to cope with future challenges. In a stable and constant technological and operating environment, such extrapolation is served by the concept of derivative design and best practices. However, in case of innovation, additional functionalities and (legal) changes in the operational environment, such a concept is questionable with respect to its validity boundaries. Theories and models may be confronted with their limitations by hidden assumptions, simplifications and extrapolations beyond their original specifications and contexts. In such cases of a disruptive approach, also the knowledge bases and repositories are to be scrutinized. Unfortunately, such scrutiny is fueled by hindsight from findings from safety investigations, forensic engineering analysis and risk acceptance considerations. As stated by a senior aviation safety investigator: it is the assumption that kills you (or users, your crews and passengers).

Based on a series of investigations, deficiencies in safety critical knowledge and safety knowledge management were identified in several major events in transport, logistics and infrastructure. This contribution elaborates not only on contributing factors and conditions during safety events. It primarily explores systemic aspects and levels that are beyond the visible scope of regular accident investigation practices. Change drivers, market developments, legal frameworks, governmental arrangements, policy demands on green sustainability and circular economy represent hidden complexities and

couplings behind the horizon in life cycle , short and long term systems developments. Such dynamics require Foresight, Precaution and Prospective systems design and development, integrating content and process simultaneously in the architecture of systems from a multi-actor and stakeholders perspective. Such dynamics require teaching young safety and risk professionals new (designing) tricks of the trade in both theoretical and practical professional performances in order not to forget the lessons already learned by previous generations of safety and risk engineering professionals from tragic outcomes in the past. This contribution extrapolates several 'lessons learned' by asking provocative questions about energy transition developments on land, at sea and in the air, in particular with respect to nowadays wind turbine upscaling and deployment. In order to secure the planet for future generations, a systemic Generative Design Perspective is proposed, rather than restoring -if possible at all- the damage done by Regeneration, Resilience Engineering and Recovery in its existing operating envelope.

2 Retrospections

A retrospection on the notions of safety and risk demonstrate a gradual paradigm shift from accident investigation and event analysis to safety management strategies and organizational change at the corporate level. Inherently, a shift occurred from an engineering dominance to managerial and organizational perspectives, supported by the introduction of a series of new notions and schools of thinking. Several 'belief' systems were introduced to support such a transition into 'socio-technical' system thinking. Simultaneously, social scientists raised doubts about a scientific validity of safety as a science, questioning notions of 'cause' and 'prevention', in favor of an operational risk management paradigm (Safety Science 2017). New sets of tools, techniques and theories were developed, such as Key Performance Indicators, data analysis models such as FRAM and STAMP, system models such as Cynefin, Resilience Engineering theory and democratic participation of operators by Work as Done versus Work as Imagined contradictions, weak signal detection and organizational learning. Such theories were favored by a diversion from cause towards consequences, depriving control over occurrences. An undefined and compiled notion of 'complexity' generated a disguise to understand 'emergent properties' -as defined by Rasmussen-, and dynamics of 'complex systems with tight couplings' as defined by Perrow-, which might -according to Turner-, create a 'drift into failure' due to 'human error' as defined by Reason, causing Perrows' 'normal accidents'. An exclusive control over organizational safety performance by corporate management replaced comprehension and oversight, sharing an undefined responsibility to evade liability and accountability. According to Farrier, introducing such new concepts such as Safety Management Systems, Safety Cases and State Safety Programs puts the two principles of safety management and safety investigations in opposition instead of leveraging their respective advantages. By discarding safety investigations from the analytical toolkit, such safety investigations are expelled from foresight and forced into a role of adversary whistle blowers. This discarding has three serious consequences. First, a consensus based interpretation of findings based on investigative reconstruction of events is no longer connected with managerial

responsibilities and intervention strategies. Second, investigative recommendations based on these findings are no longer incorporated in their specific corporate, stakeholder and governmental context. As stated by Hollnagel, 'in the learning process, one should learn from what went right, not from what went wrong'. In losing oversight over the context specific setting, design trade-offs and operational feedback on a triggering event, remedial control options are lost as well, both for the event as well as the system itself. Third, if no lessons learned are drawn from previous life cycle phases or are expelled from the knowledge repository, undesirable events will manifest themselves as 'emergent properties' rather than system inherent properties, designed into the system. Such events stem from previous design requirements, optimization considerations and trade-offs. Clarifying such decisions and subsequent properties should be part of the investigative process and system diagnosis. Otherwise only rescue, recovery and resilience approaches are available in the aftermath of events to remedy system deficiencies in a strict retrospective manner. Since an equivalent of Environmental Impact Assessment legislation does not exist for assessing integral safety in transport, logistic and infrastructure project decision making, the only option is to develop an engineering design methodology, incorporating the safety dimension (TCI 2004).

A first conclusion is that a dialectic stall in scientific notions and knowledge occurred during this transition. Derivative approaches from socio-psychological and organizational disciplines provided an anti-these for the technological engineering design theses, but were not able to deliver a synthesis in a scientific paradigm shift for safety thinking in (design) context and operational environment

3 An ESReDA remedial response

An ESReDA remedy response to this stall preferred a disruptive approach which, according to Vincenti (1990), might perform better than derivative adaptations and linear extrapolations, given the changes in the operating environment. Socio-economic and technological environments change according to market development, governmental (legal)arrangements and public-policy demands. Such changes are triggered by societal demands on circular economy, climate responsive changes, proactive adaptation and regenerative design options to accommodate 'foresight and providence' in a neo-liberal economy (ESReDA 2020).

A second conclusion is the necessity to develop a new systems methodology: incorporating safety investigations, user knowledge based and value chain based system design and operations.

To facilitate foresight, a stepwise approach should be favored: first understand, then comprehend, explore beyond the event and add system architecture, complexity and dynamics to the analysis, provide a timely transparency in the factual functioning of the (sub)systems, and diagnose system problems to identify solution spaces beyond the event level during operations.
To enable such a disruptive system approach, two primary conditions have to be fulfilled:

- explore the basics of a safety investigation methodology
- Identify the assumptions, (design) knowledge deficiencies and correlations in the subsystems.

During the journey of several ESReDA working groups, the safety investigative methodology and processes have been unraveled and structured to fulfil the first condition.
The *investigation processes* contains 3 phases:
1. The investigative reconstruction of the event in its environment
This phase contains a factual description of the system components, aspects and dimensions to facilitate the step from description to explanation of the event in its context, given the available data and operational conditions
2. The analytic interpretation of facts and findings
This phase is mobilizing knowledge and expertise about states, deficiencies, design and operational assumptions, models, simplifications, interactions to facilitate the step from understanding to sustainable change and performance enhancement: foresight by hindsight and insight.
3. The adaptive intervention by learning, recommending and change
This phase is categorizing change options in the event and the system as derivative, disruptive or prospective adaptations, applying system engineering design and change management principles to facilitate the step from recommending to implementing knowledge and value based solution spaces and operational envelopes.

The adaptive intervention copes with the *system architecture, -complexity and -dynamics*. To address these characteristics, during the system analysis, efforts should be dedicated to clarify the system-constraints itself:

- Change the focus to conceptual change rather than form and function variation
- Identify assumptions, simplifications and extrapolations
- Identify knowledge deficiencies in design expertise and operational experiences
- identify and validate system boundaries: technological, social, institutional, ecosystem
- Identify the operating envelope, also on the long term
- Apply the full information paradigm: combine feedforward and feedback
- Lessons learned or lessons forgotten, denied or dismissed
- Identify political-societal change agents, change drivers and bifurcation, subsystem points.

Putting events in their systemic context and operating envelope facilitates an assessment of the event as a ‘normal’ accident within or outside the intended design and operating envelope. Recommendations on remedies for such events may reflect a necessity to make derivative or disruptive adaptations during subsequent system revisions.

A third conclusion is to develop a Prospective, Future Proof approach, by Foresight and by ~~a~~ Generative Design Methodology, on land, at sea and in the air. Does this approach foresee future safety performance without abundant feedback from safety occurrences?

4 The windturbine energy case study

In this contribution, wind turbine energy transition practices during the 2030 – 2050 period in the Netherlands are applied to demonstrate the distinction between event safety investigations and system safety investigations. Since hardly any safety related events have occurred during the introduction of wind turbine generated energy transition process, safety has been absent in the public debate and governmental and policy making processes. Rather than based on factual information and system based analysis, safety assumptions have been made, based on 'belief' systems and minor collateral damage assumptions, such as collisions with bats and birds, noise abatement and flickering shadow nuisance. Wind turbine inherent technical safety aspects are considered proprietary expertise and are left out of the equation in the public debate. Safety is reduced to 'external safety' as an environmental component and assessed as a public perception issue (Weteringe 2023, Elze van Hamelen 2024). Basic scientific domains such as aerodynamics, meteorology, geophysics and acoustics are not admitted to the public debates and considered proprietary expertise of turbine manufacturers, while democratic participation, sustainability, operating envelopes and operating conditions are not taken into account. Publicly accessible data registration systems are fully absent. Instead, linear extrapolations of turbine dimensions, power generation, spatial planning and land use issues are preferred by the turbine industry: 'bigger is always better'. This assumption however, proves to be questionable (GCube 2023). Performance standards on noise and nuisance and environmental impacts in the public domain are submitted to legal, ad-hoc procedures and judicial verdicts as the basis for a public debate in a massive deployment of this high energy density industry.

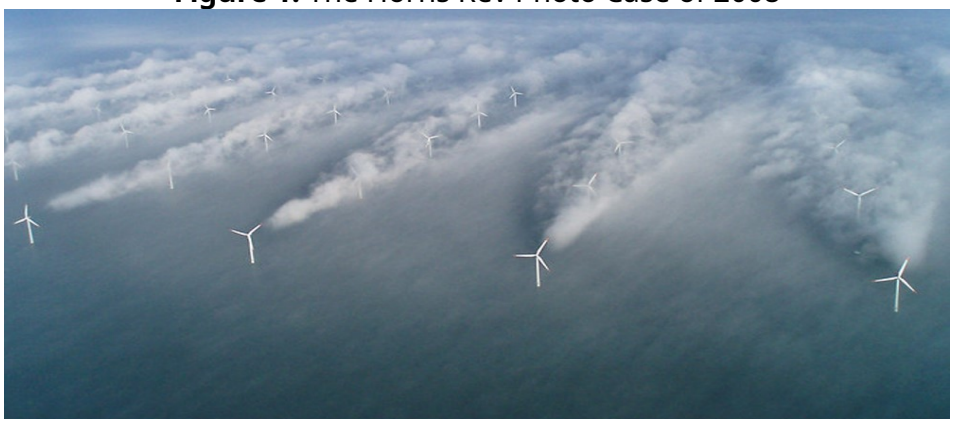
Pilot holes Wind turbine farm anomaly

According to insurance market experts, there has been a rapid commercialization of 'prototypical technologies', by an accelerated leap in turbine dimensions and performance from a 3-8 MW to a 8-18 MW category of turbines. This leap creates financial pressure on manufacturers, supply chain and insurance markets. The industry is

reaching a vertical limit, where the 'bigger is better' assumption is to the detriment of safety, quality, reliability and sustainability (GCube 2023). Could this have been foreseen by mobilizing knowledge from scientific domains and research institutes that were not involved in the public debate? Was the knowledge already 'in the market', similar to experiences in high tech industries such as aviation and maritime or were new entrants in the industry dominant in a 'hard' insurance market with increasing risks and losses?

Finally, what are the consequences of extracting huge amounts of energy from the lower levels of the atmosphere? The impact of such a large scale extraction of energy on weather and climate conditions has hardly been explored. New phenomena are emerging, such as pilot holes and wind turbine farm anomalies in various layers of the atmosphere. Are such anomalies accidental emergent phenomena, only observable in practice, to be labelled as 'serendipities', such as the Horns windfarm case in Denmark? Do they represent new unforeseen inherent properties, challenging the assumptions on the adiabatic nature of atmospheric processes?

Figure 1. The Horns Rev Photo Case of 2008



A Quick Scan on scientific literature on satellite observations, aerial photography and climate modelling reveals a wealth of experience and expertise, directly accessible in geosciences, meteorology, climate change and energy transition literature (Klotzbach et.al. 2009, Miller et.al. 2011, Hasager et.al. 2013). Such scientific knowledge indicate the limits of growth of energy transition challenges, uncertainties and deficiencies in large scale wind farming developments. Such knowledge was foreseeable at the practical introduction of major windfarm initiatives since the 2010's, but not explored, leaving windfarming a 'perpetuum mobile' (Kleidon 2021). It assumed windfarming an unlimited source of energy, ignoring thermodynamics, geosciences, meteorology and aerodynamics knowledge domains. In particular the role of turbulence and dynamic interactions between the inner and outer layer of the atmospheric boundary layer is to be scrutinized in order to understand the recovery of the energy content of the boundary layer after the 'harvesting' of kinetic energy by wind turbines. Such harvesting impacts the humidity, precipitation, temperature, velocity and pressure, which requires downstream airflow recovery distances of hundreds of kilometers. Mutual windfarm interactions by wake propagation is significant and influences energy production efficiency over long distances (Baas 2024).

A fourth conclusion is that a systemic analysis reveals that each of these performance aspects contain knowledge deficiencies, unvalidated assumptions and undisclosed

subsystem correlations. Primary system safety characteristics however, are hardly addressed.
A system analysis reveals deficiencies and serve as a foresight enabler before the turbine industry has reached maturity. Such a disruptive introduction of systems approach in the analytic diagnosis of events however, is not enough to accommodate foresight in technological innovation and system transition challenges. To achieve a prospective approach in complex and dynamic socio-technical systems, principles of First Time Right and Zero Defect should be applied. However, such an approach does not yet exist in transportation systems design (TCI 2004). Transportation systems are characterized as High Energy Density Systems and are 'never dying systems' due to their 24/7 operational availability in open access, global networks. In addition they are characterized by a constant change in technology, organization, control and legislative arrangements and hybrid nature during transition periods. Designing such transportation, infrastructure and logistic systems in a sustainable, future and climate robust manner, requires the development of foresight enablers, developed as specific notions, tools and proactive assessment techniques, in a context of institutional arrangements, supranational oversight and governmental control mechanisms. The wind turbine industry should also adhere to such a systemic approach, belonging to the High Energy Density system category.
This contribution indicates several perspectives and conditions under which such a toolkit can be used to design the future. These perspectives are derived from engineering design methodologies and safety science as developed in aviation, the maritime and agricultural domains.

5 Towards a generative design perspective

5.1 Foresight enablers

In this contribution two enablers of foresight are elaborated:

- Forensic engineering and safety investigations
- Socio-technical system engineering design methodologies.

These enablers are materialized by the introduction of a new system design perspectives, four new tools and identification of key success factors. Such enablers facilitate the expansion of the design envelope in both a horizontal and vertical direction. The horizontal expansion of the design envelope copes with an integral approach of all relevant design aspects, matching 'hard' and 'soft' design requirements alike. The vertical expansion copes with higher order system requirements, such as dynamic-adaptive anticipation of future priorities and robust, future proof frameworks. For each of these expansions and adaptations of the design methodology, specific tools are developed. Additional disciplines and actors are introduced, each with their preferred values, goals and disciplinary knowledge and expertise. Such an approach requires the (re-) introduction of a systems architect in the role of a system integrator being an initiator of cooperation and communication (TCI 2004).

First, forensic engineering and safety investigations as foresight enablers require a stepwise upgrade of the factfinding phase of the investigation process from the single event to the level of system design and operations. Such a factfinding mission starts with identification of single issue safety aspects and is data driven. Such a mission focuses on derivative form variations, deviant or normal, related to the intended design parameters and assumptions. During the analysis and interpretation of the findings of this mission, multiple issues can be explored, driven by business model considerations, balancing

various aspects of a People, Profit and Planet based nature. This investigation phase considers the impact of disruptive functionalities on the subsystem level and their appearance during intended operations.

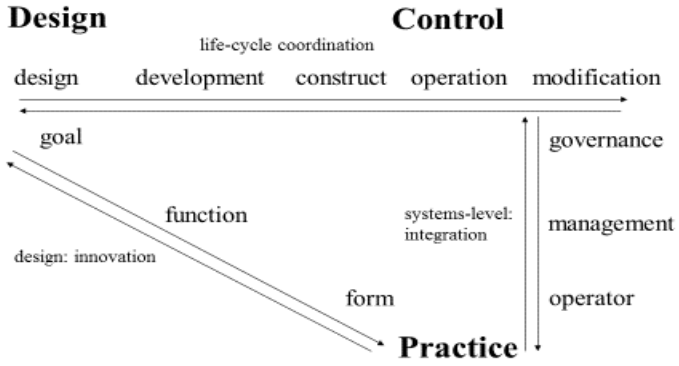
Second, based on socio-technical systems engineering design methodologies in various transportation and infrastructure domains, Knowledge Based and Value Based driven considerations are to be identified. They serve as triggers for change and adaptation to redesign the system as compatible to modifications in goal based concepts, future proof and climate change. Analyzing the potential of a prospective 'foresight' approach, the expansion of the analysis to higher system levels and objectives creates a reference framework for the analysis of the event. In this framework, the assumptions, limitations, interactions and correlations across the system as a whole can be identified. The analytic focus expands from an operational event reconstruction towards a life cycle based system approach, covering design, development and operations. A transfer occurs from a static-reactive focus towards a dynamic-adaptive focus, anticipating future priorities and transition robust frame works (Safety Science 2017).

5.2 New tools

To facilitate such a transition in upgrading diagnostic potential to the system level, four new tools were developed to provide structure and control mechanisms to guide the design process:

1. The Design – Control – Practice diagram. This diagram puts the design, control and practice interrelations in a systemic context. The system life cycle provides relations between design, development, construct and operation to adaptation and decommissioning. The systems level of control relates operator compliance with management control and governmental oversight at the micro, meso and macro level. The engineering design cycle deals with successive design phases of goal, function and form. The diagram allocates positions of methods, tools and techniques, enabling a navigation through the safety landscape and their solution domains.

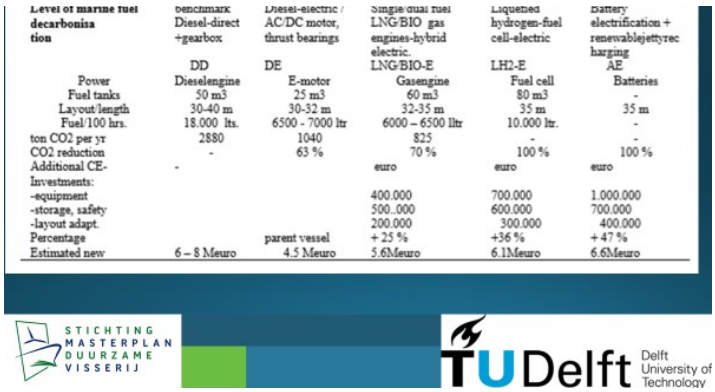
Figure 2. The DCP diagram



2. the CEDI sustainability matrix (Veenstra 2024) identifies the primary design dimensions and their hard as well as soft performance parameters which are to be

incorporated in the Program of Requirements and are to be specified and allocated to modular design subsystems.

Figure 3. The CEDI matrix

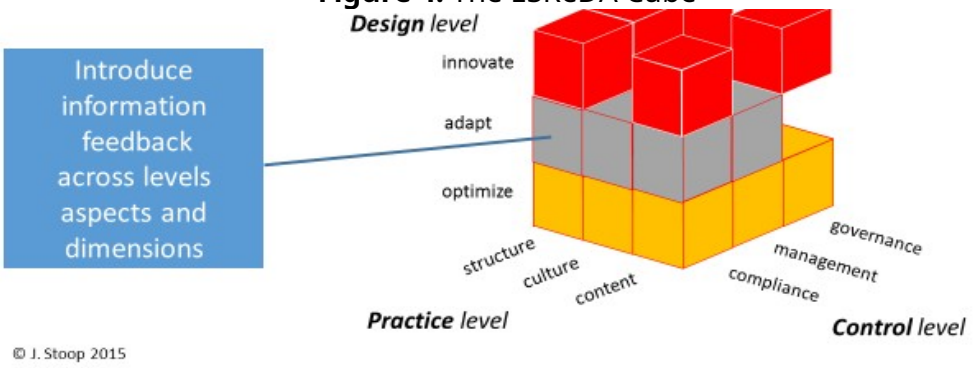


Level of marine fuel decarbonisation	benchmark Diesel-direct +gearbox	Diesel-electric / AC/DC motor, thrust bearings	Single/dual fuel LNG/BIO gas engines-hybrid electric.	Liquefied hydrogen-fuel cell-electric	Battery electrification + renewablejettyrecharging
	DD	DE	LNG/BIO-E	LH2-E	AE
Power	Dieselengine	E-motor	Gasengine	Fuel cell	Batteries
Fuel tanks	50 m3	25 m3	60 m3	80 m3	-
Layout/length	30-40 m	30-32 m	32-35 m	35 m	35 m
Fuel/100 hrs.	18.000 lts.	6500 - 7000 ltr	6000 – 6500 ltr	10.000 ltr.	-
ton CO2 per yr	2880	1040	825	-	-
CO2 reduction	-	63 %	70 %	100 %	100 %
Additional CE-Investments:	-		euro	euro	euro
-equipment			400.000	700.000	1.000.000
-storage, safety			500..000	600.000	700.000
-layout adapt.			200.000	300.000	400.000
Percentage		parent vessel	+ 25 %	+36 %	+ 47 %
Estimated new	6 – 8 Meuro	4.5 Meuro	5.6Meuro	6.1Meuro	6.6Meuro

This CEDI approach is a system-design methodology taking into account business and climate responsive design choices in the early design phase, like here for an engine room subsystem. The CEDI index explores which sustainable solutions are becoming available in the chosen timeframe 2030-2050. By ranking (semi)proven, rapidly emerging green technologies, the linear MDV-1 design process is evolving into a more flexible modular and circular MDV-1 design process with, for short and long term change potentials the estimated subsystem refitting costs.

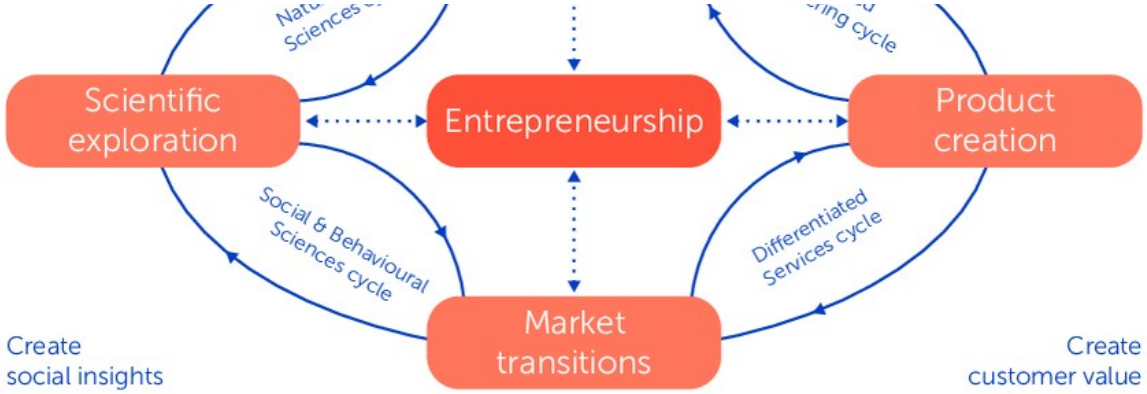
3. The ESReDA cube aims at bridging the gap between interpretation and intervention by application of design principles, control strategies and over various aspects of evidence and information on knowledge based solutions concerning the structure, context and content of design and control over operational processes.

Figure 4. The ESReDA Cube



4. The MCIM model serves as a technical-social-customized model, identifying the necessary cooperation between scientific, technical, product and market dimensions in order to achieve a successful introduction of cyclic innovative processes and products.

Figure 5. The MCIM model



Throughout several PhD projects in transportation and major infrastructure initiatives in the Netherlands, a series of critical key success factors were identified:

- Apply a safety and sustainability problem orientation
- Share knowledge with participatory choices regarding modelling, functionality and goals
- Identify assumptions, limitations and simplifications
- Communicate and coordinate across users and multi-stakeholders
- Generate component innovations, subsystem optimization and overall system concept integration
- Acknowledge safety investigators as system architect counterparts.

6 Conclusions

A Fifth conclusion can be drawn from the experiences with successively applying knowledge and value based design in aviation, flexible modular and sustainable design in the maritime industry and regenerative design methodologies in agriculture sector. Foresight cannot be achieved with such methodologies in isolation. A future proof and change robust systems design requires a new, prospective design paradigm, combining elements of engineering design methodology, change, adaptation and foresight.
Rather than continuing a stalled debate across disciplines, stakeholders and perspectives, a synthesis of notions, theories and intellectual constructs is required. To foresee a future functioning of manmade artefacts, safe and sustainable. A main prerequisite is to provide transparency for each of the disciplines and perspectives.

This paper extrapolated the 'lessons learned' from transport, infrastructure and logistic system engineering designs to the energy transition and wind farming developments in the Netherlands. Taking into account the system architecture at all levels and aspects, four new tools could be applied. From a Generative Design Perspective the case study results in three provocative questions on developments on land, at sea and in the air:

- On land: questions are raised in the public debate about land use planning and environmental policy making with respect to location and configuration selection

criteria regarding integral safety and risk perception of large turbines and their local *wind climate* impact in the lower atmospheric boundary regions

- At sea: questions are debated in aerodynamic research and engineering communities which are hardly communicated with public and governance entities, regarding wake and turbulence interferences within and across wind farm dimensions and locations, causing efficiency losses and their impact on *weather changes* in the downwind dispersion of their effects in the upper parts of the atmospheric boundary regions
- In the air: questions are debated in geophysical and meteorological communities regarding the total solar energy influx balance, its dissipation across atmospheric and maritime modes, their inherent physical limits for energy transition goals and the impact om *climate changes* in the long term at the global level.

Reducing these questions to a debate on benefits of wind farming in general according to a 'bigger is better' and a 'race to scale' level is applying a 'Procrustean Bed' solution: an arbitrary standard forcing anybody to an exact conformity.

Finally, the future begins at investigating current deficiencies in system design methodologies in order to eliminate their inherent assumptions, limitations and simplifications and to achieve foresight over future developments. The new EU Directive on Resilience of Critical Entities , combined with the new school of safety thinking in Generative Design Perspectives may support such foresight, otherwise these deficiencies will kill you.

Acknowledgements

In addition to these key references, many papers and presentations are provided by the PhD graduates in the transportation and infrastructure safety domain. Without their contributions, this paper would not have been written. In alphabetic order; Wim Beukenkamp, Geert Boosten, Arthur Dijkstra, Erik van Kleef, Frederic Mohrmann and Frans Veenstra.

References

Baas P. 2024. Winds of the North Sea in 2050 – Public Final Report Whiffle, Delft, the Netherlands

Elze van Hamelen 2024. Het Windmolendrama. Hoe de uitrol van industriële windturbines een nieuwe toeslagenaffaire dreigt te worden. Clintel 2024 (in Dutch)

ESReDA 2020. Enhancing safety: the challenge of Foresight. ESReDA Project Group *Foresight in safety,* EUR 30441 November 2020

EU 2024. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Hasager C. et.al. 2013, Wind Farm Wakes: The Horns Rev Photo Case. Energies, 2013, 6, 696-716, ISSN 1996-1073

Kleidon A. 2021, Physical limits of wind energy within the atmosphere and its use as renewable energy: From the theoretical basis tp practical implications. Meteorological Zeitschrift, July 2021

Klotzbach P. et.al. 2009, An alternative explanation for differential temperature trends at the surface and in the lower troposphere. Journal of Geophysical Research, Vol 114, D21102, 2009

Miller L. et.al. 2011. Estimating maximum global land surface wind power extractability and associated climatic consequences. European Geosciences Union, Vol 2, Issue 1, ESD 2, 1-12, 2011

GCube 2023. Vertical Limit: When is bigger not better in offshore wind's race to scale? GCube Renewable Energy Insurance. Q2 2023 Report

Safety Science 2017. A founding fathers' retrospection. Stoop J.A., De Kroes J.L. and Hale A.R. Safety Science 94, (2017) 103 - 115

TCI 2004. Veiligheidsborging van grote infrastructuurprojecten. Tweede Kamer der Staten Generaal. Vergaderjaar 2004 – 2005. KST85060 ISSN 0921 - 7371 Sdu Uitgevers's-Gravenhage 2005 (In Dutch)

Veenstra 2024 Toekomstbestendig ontwerpen, Visserij duurzaamheid en systeem methodische ontwerpprocessen. Wageningen University, the Netherlands (In Dutch, English summary available)

Weteringe B. 2023. Windhandel De impact van grootschalige energieopwekking met windturbines. Obelisk Boeken Nl (in Dutch)